REMARKS

Claims 1-13, 15-18 and 21-28 are pending in the application. Claims 1-13, 15-18 and 21-28 have been rejected. Claims 1, 2, 8-13, 15, and 24-28 have been amended. No new matter is added.

Telephone Conversation With Examiner

Examiner Perungavoor is thanked for the telephone conversation conducted on October 10, 2008. Proposed claim amendments were discussed. Cited art was discussed. Examiner Perungavoor indicated that, as he interprets the claims as amended, one algorithm is being replaced with another, and that this, alone, does not overcome the cited art. Applicants' representatives explained that the claims are not directed to merely replacing algorithms. Applicants' representatives agreed to amend the claims to more clearly indicate this.

Initial Matters

On page 2, the Office Action provides the standard form paragraph regarding an obviousness rejection under 35 U.S.C. 103(a). However, the heading for the rejection recites "Claims 1-2, 7-9, 24-26 are rejected under 35 U.S.C. 102(b) as being anticipated" which provides some confusion as to the intention of the Office Action. Clarification on the record is respectfully requested. Applicant's Representative will assume in the following response that the rejections set forth in the Office Action are based in 35 U.S.C. 103(a) and are based upon obviousness, not anticipation, of the enumerated claims.

Claim Rejections Under 35 U.S.C. § 101

Claims 8-13 and 24-28 are rejected under 35 U.S.C. § 101 because they are allegedly directed to non-statutory subject matter. Without prejudice or disclaimer, claims 8-13 and 24-28 have been amended to recite a "computer readable storage medium." Accordingly, it is

requested that the rejection of claim 8-13 and 24-28 under 35 U.S.C. § 101 be reconsidered and withdrawn.

Regarding the Rejections under 35 U.S.C. §103

Claims 1-2, 7-9, and 24-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over "RFC-3244-Microsoft Windows 2000 Kerberos Change Password and Set Password Protocols", Swift et al. (hereinafter "Swift") in view of Hussain et al. (US Patent Publication 2004/0205331, hereinafter "Hussain"). Claims 3-6, 10-13, 15-18, 21-23, and 27-28 are rejected in view of Swift, Hussain and further in view of "rpcsec_gss, kadmin service principal, etc", Coffman. Swift is directed to the process of specifying, setting and resetting passwords within the Windows 2000 implementation of the Kerberos change password protocol that interoperates with the original Kerberos change password protocol. Hussain is directed to an apparatus and method for allocating resources within a security processing architecture using multiple groups. Coffman is directed to the use of the GSS API in the specification of Kerberos protocol based systems. These rejections are respectfully traversed.

The claimed subject matter relates to the encryption algorithm negotiation in the context of encryption-based authentication protocols. In Applicants' Application, a system and method is provided that need not interfere with the standard operation of existing authentication protocols. A first computer sends a negotiation request to a second computer after the establishment of a network connection between the two computers in which the negotiation request specifies that the first computer supports a selected encryption algorithm. The second computer may return a subsession key for encryption using the selected encryption algorithm. Both first and second computers may then switch to encryption in the selected encryption algorithm, using the subsession key to encrypt future communications.

Regarding claims 1 and 8, claim 1 recites "sending a subsession key to the client computer, wherein the subsession key may be used by the client computer to switch from an

established first encryption to a second encryption algorithm for use in conjunction with the selected encryption algorithm to encrypt future communications to the server computer" and claim 8 recites in part, "switching to the specified encryption algorithm if the subsession key for use with the specified encryption algorithm is delivered." The Office Action admits on Page 2 that Swift does not teach or disclose the negotiating of encryption algorithms. Applicants agree. In addition, it is submitted that Swift also does not teach or disclose "switching to the specified encryption algorithm" in any form, which is recited in part in claims 1 and 8 and is a separately patentable distinction between Swift and the claims.

It is respectfully submitted, that Swift is being mischaracterized in the Office Action. The Office Action asserts that Swift discloses or teaches "switching to the specified encryption algorithm if the subsession key is delivered" on page 3 of the reference, however, it does not. Swift, on page 3, discloses the process for changing a password after an authenticated password has been generated and a subsession key has already been assigned. There is no "specification of encryption" of any kind in Swift, and the only mention of encryption is that an encryption algorithm is used to decrypt the password from the first (client) computer. Thus, Swift is silent on "switching to the specified encryption algorithm" as recited in claims 1 and 8. Swift is also silent with regard to switching from one encryption algorithm to another after the initial network communication is established between a first computer and a second computer as recited in "wherein the subsession key may be used by the client computer to switch from an established first encryption to a second encryption" in claim 1, and by "sensing an encryption algorithm negotiation request to a server computer indicating that a client computer in current communication with the server" in claim 8. Thus, Swift does not disclose or suggest at least the above recited subject matter of claims 1 and 8.

The Office Action looks to Hussain to cure the deficiencies of Swift, however, it does not. Hussain discloses in paragraphs [0005] – [0007] only that the encryption parameters are exchanged initially to establish a secure session for communications between two computer systems. There is no disclosure or suggestion of switching from one established encryption to a second encryption algorithm after a secure session has been established as recited in claim 1, nor

is there any disclosure of a subsession key transmitted or received from one computer to another subsequent to the establishment of a secure session as recited in claims 1 and 8. Thus, the combination of Swift and Hussain does not provide the teaching to render claims 1 and 8 obvious. Reconsideration and allowance are respectfully requested.

Claim 24 recites "reading a negotiation request from a first computer, wherein said negotiation request is a negotiation request subsequent to transmission of a subsession key by the first computer and specifies one or more encryption algorithms supported by the first computer, and wherein the negotiation request is included with an authentication protocol communication from the first computer." Swift is silent with regard to this subject matter. The Office Action looks to Hussain in paragraph [0006] to disclose the negotiation of encryption algorithms subsequent to the communication of a subsession key and the transmission of a subsession key, however it does not. Hussain, in paragraphs [0005] – [0007], discloses the initial generation of a secure session between two computer systems, including the selection of an encryption algorithm. However, once the initial session is established, there is no further negotiation between the two computer systems. This is not the same as the recited features of claim 24. In the claim, a subsession key may be transmitted from one computer system to another to establish a new type of secure encryption on a temporary basis and thereafter attempt to specify a new, different encryption algorithm for future communication between the two computers. The combination of Swift and Hussain does not disclose or suggest the subject matter of claim 24. Reconsideration and allowance are respectfully requested.

Claim 15 recites "including an automatic renegotiation request for an encryption algorithm with an authentication protocol process communication from the first computer to the second computer, wherein the renegotiation request specifies that the first computer supports one or more encryption algorithms." The Office Action asserts that the combination of Swift and Hussain discloses this subject matter, specifically in paragraph [0006] of Hussain, however, it does not.

Once again, Swift is silent with regard to the renegotiation of encryption algorithms of any type, and Hussain discloses only that encryption algorithm information may be exchanged to select an initial algorithm for use upon the establishment of a secure communication channel between two computers. There is no disclosure in either reference for the renegotiation of encryption algorithms once a secure communication channel is in place. Coffman, included for its disclosure of a "gss interface," is also silent with regard to the renegotiation of encryption algorithms as recited in claim 15 and thus does not remedy the lack in Swift and Hussain. Thus, the combination of Swift, Hussain, and Coffman does not provide the disclosure necessary to render claim 15 obvious. Reconsideration and allowance are respectfully requested.

Claims 2-7, 9-14, 16-23, and 25-28 all depend, either directly or indirectly, from one of claims 1, 8, 15, and 24. As such, the applicants submit that these claims are patentable over the combination of Swift, Hussain and Coffman for at least the same reasons as stated above with respect to claims 1, 8, 15 and 24. Accordingly, reconsideration and allowance are respectfully requested.

Further, a *prima facie* case of obviousness has not been established because support for obviousness comprises only conclusory statements. A *prima facie* case of obviousness has not been established because it has not been explained why one of skill in the art at the time of the claimed subject matter would have been motivated to combine Swift and Hussain. And, it has not been explained how Swift and Hussain would be combined to arrive at the claimed subject matter.

The MPEP provides several guidelines for rejecting a claim under 35 U.S.C. 103(a). Specifically, reference is made to MPEP § 2141. III - Rationales To Support Rejections Under 35 U.S.C. 103, which states in part:

> "Office personnel must explain why the differences(s) between the prior art and the claimed invention would have been obvious to one of ordinary skill in the art. … The key to supporting any rejection under 35

> U.S.C. 103 is the clear articulation of the reason(s) why the claimed invention would have been obvious. The Supreme Court in *KSR* noted that the analysis supporting a rejection under 35 U.S.C. 103 should be made explicit. The Court quoting *In re Kahn,* 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006), stated that "'[R]ejections on obviousness cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.'" *KSR*, 550 U.S. at ___, 82 USPQ2d at 1396." (Emphasis added)

Additionally, the Examiner should explain how to combine the references, per MPEP 706.02(j).

> "35 U.S.C. 103 authorizes a rejection where, to meet the claim, it is necessary to modify a single reference or to combine it with one or more other references. After indicating that the rejection is under 35 U.S.C. 103, the examiner should set forth in the Office action: (A) the relevant teachings of the prior art relied upon, preferably with reference to the relevant column or page number(s) and line number(s) where appropriate, (B) the difference or differences in the claim over the applied reference(s), (C) the proposed modification of the applied reference(s) necessary to arrive at the claimed subject matter, and (D) an explanation >as to< why >the claimed invention would have been obvious to< one of ordinary skill in the art at the time the invention was made**." (Emphasis added)

Further, when explaining how to modify a reference, "the proposed modification can not render the prior art unsatisfactory for its intended purpose" (MPEP 2143.01.V), and "the proposed modification can not change the principle of operation of a reference. (MPEP 2143.01.VI).

CONCLUSION

For the forgoing reasons, Applicants respectfully submit that the instant application is in condition for allowance. Reconsideration and early allowance is hereby respectfully requested.

Date: October 15, 2008

/Joseph F. Oriti/
Joseph F. Oriti
Registration No. 47,835

Woodcock Washburn LLP
Cira Centre
2929 Arch Street, 12th Floor
Philadelphia, PA 19104-2891
Telephone: (215) 568-3100
Facsimile: (215) 568-3439